TELEMATIQUE Volume 21 Issue 1, 2022
ISSN: 1856-4194 5800 – 5809

Mystalk Alert: A Response to Cyberstalking in Malaysia

Wan Rosalili Wan Rosli[1*], Saslina Kamaruddin[2], Ahmad Ridhwan Abd Rani[3], Nadia Nabila Mohd Saufi[4], Nur Masharah Husain[5]

[1*]School of Law, Faculty of Management, Law and Social Sciences, University of Bradford, United Kingdom
[2]Faculty of Management & Economics, Sultan Idris Education University, Perak, Malaysia
[3]Universiti Teknologi MARA,Shah Alam, Selangor, Malaysia
[4]Faculty of Business Management & Professional Studies, Management & Science University, Selangor, Malaysia
[5]Faculty of Art, Computing Creative Industry, Sultan Idris Education University, Perak, Malaysia

Email id: [1]w.r.wanrosli@bradford.ac.uk

Received 10/09/2022; **Accepted** 04/10/2022

Abstract:
The Internet has become a vital part of our daily lives in the last two decades. However, as a double-edged sword, such reliance has increased the chance of being targeted by various cybercrimes, including cyberstalking. Furthermore, when the crime transcends into the real world, it can result in rape and even murder. Hence, the MYStalk Alert application aims at helping and facilitating the victims of stalking and victims of harassment generally to understand, cope, and document their experience on the crime for a compelling trail of evidence in the criminal justice process. This Application aims to remedy the circumstances by giving access to users to the features that make it easy to document the evidence and provides them with available information on the crime and the legal landscape of stalking in Malaysia. Furthermore, MYStalk Alert also focused on the user's physical and psychological by providing self-assessment and tips for the wellbeing including mental health test under the feature of victims' support. The Application is a first of its kind in Malaysia and aims to support victims of stalking in getting the justice they deserved. The preliminary findings revealed contradictory views on the effective response of the criminal justice system towards cyberstalking, which explains the under-reporting of such crime. Significantly, the findings illustrate that the current Malaysian legal framework on cyberstalking is deficient in protecting cyberstalking victims, which calls for an urgent need for a review in the Malaysian laws.

Keywords: Cyberstalking**,** Cyberspace, Criminal Justice, Risks, Victimisation

1. INTRODUCTION

Harassment and stalking in real life have become commonplace during the last two decades. The emergence of the dark side of such crime has been aided by the introduction of information and communication technology (ICT), particularly the Internet and its applications, such as the social media platform. It has now transgressed into cyberspace and is now deemed to be more hazardous when committed online, as it was once perpetrated in the physical world. In terms

of the prevalence of such crime, MyCERT incident reports show that cyber harassment incidents, such as cyberstalking, have increased significantly in the last six years, indicating the rising threats that the crime poses to Malaysians. It has now made its way into cyberspace, where it is now deemed to be more damaging than when it was done in the physical world. The existing research on cyberstalking argues that the veil of anonymity attracts stalkers to stalk their victims in cyberspace on a global scale (Fissel & Reyns, 2020, Kalaitzaki, 2020, Ahlgrim, 2015, Heinrich, 2015, Middlemiss, 2014). According to Papakitsou (2020), Leong (2015), Reyns (2019), and Tavani and Grodzinsky (2002), Internet anonymity allows cyberstalkers to operate anonymously or pseudonymously, allowing them to stalk several victims from the comfort of their homes without having to leave the house. Traditional stalking and cyberstalking studies have revealed that women are more likely to be stalked than men, implying that such crime is primarily a gender-motivated crime committed by men against women (Godwin, 2003, Medlin, 2002, Reyns, 2019, Nobles, 2013).

Currently, real-life stalking as well as cyberstalking are both illegal in many places throughout the world. In 1992, California became the first state in the United States to make stalking illegal (Vasiu and Vasiu, 2013). Anti-stalking legislation was introduced in 1997 in England and Wales and New Zealand, respectively, under the Protection from Harassment Act (PHA) 1997 and the New Zealand Harassment Act 1997. Both criminal and civil harassment are covered by these laws (CCPL, 2013). Singapore followed the lead of the English and Welsh in criminalising cyberstalking in 2014, enacting the Protection from Harassment Act (Hamin & Wan Rosli, 2016 & 2020). Anti-stalking laws in England and Wales, Singapore, and the United States, provide numerous rights for stalking victims, including protection orders, injunctions, damages, and restraining orders (Todd, Bryce & Franqueira, 2020, Middlemiss, 2009; Cheong, 2014).

The literature on the criminalization of cyberstalking, much alone the protection of cyberstalking victims, is relatively rare in the local legal landscape. According to recent research, traditional criminal law in the form of the Penal Code and cyber law in the form of the Communication and Multimedia Act 1998 are two conceivable legal remedies to cyberstalking in Malaysia (Hamin & Wan Rosli, 2017 & 2020). Female cyberstalking victims are reluctant to disclose the offence to the authorities, according to other local literature (Haron, 2010). Similarly, according to a report by CyberSecurity Malaysia, cyberstalking is just the tip of the iceberg, and hence peripheral, because the actual number of victims is higher because not all victims are willing to come out and disclose their victimisation (CyberSecurity Malaysia, 2019). This study examines the the impact on victims' access to justice in this environment and the inadequacy of the law in addressing the crime. As a result, the purpose of this research is to provide a viable solution for the problem and also address a vacuum in the literature on cyberstalking in Malaysia.

The first part of this paper examines the legal position of cyberstalking in the existing Malaysian statute book. The second part explains the methodology adopted by the researchers in conducting the research. The third part, which is the crux of the study, explains the findings on the drivers for the underreporting of such crime, the impact on the victim's legal protection and the facilitating effect of the MY Stalk Alert App in recording trail of evidences to expediate prosecution and investigation . The discussion in the fourth section discusses the relationship between the findings and the literature before the last section concludes the paper.

Literature review

Cyberstalking is defined as a pattern of behaviour in which a person uses information and communication technologies (ICTs) such as e-mail, forums, blogs, and social networking

websites to continually harass and pursue another person, causing concern or terror in the latter (Mutawa, 2016). Cyberstalking behaviours include intimidation, accusation, surveillance, and also impersonation of the victims (Mutawa, 2016). Cyberstalking is defined by the Australian Institute of Criminology (2016) as persistent behaviours that instil dread and apprehension within a virtual setting. Smoker and March (2017) argue that cyberstalking has grown more acceptable than ever before as a result of technological advancement, which has increased avenues of communication and open access to information, as well as the potential for uninhibited behaviour in cyberspace.

According to some observers, cyberstalking may be more hazardous and frequent than traditional stalking because of the Internet's numerous crime triggers, which present significant chances for the use of powerful computer programmes (Aa, 2011; Mutawa, 2016). Cyberstalkers have no difficulty locating their victims, as it is as simple as clicking a button. The likelihood of being confronted with their acts is nil, as they will cover their identities, alter critical data, move and delete material in a matter of seconds, and destroy proof (Aa, 2011). According to Rawlinson (2015), 98 percent of domestic abuse victims in Australia have also experienced cyberstalking. According to Al-Khateeb and Epiphaniou (2016), more than 38% of cyberstalking victims fear that the offenders' aggressive behaviour online may escalate into a face-to-face encounter. Tokunaga and Aune (2015) assert that cyberstalking is a growing threat and estimate that around 20% to 40% of Internet users are victims of cyberstalking. According to the US Bureau of Justice Statistics (2017), around 14 out of every 1,000 persons aged 18 or older may become victims of cyberstalking within a year. Cyber harassment incidents in Malaysia have tripled in the previous decade, according to latest figures published by the Malaysian Computer Emergency Response Team (MyCERT) (MyCERT, 2016). MyCERT reported 406 instances of this type of crime in the first half of 2017. This indicates an increase in the number of reported cases, as 529 were reported in 2016 compared to 442 in 2015.

According to the research on the amount of female victimisation in cyberstalking, the majority of stalking victims are women, while the majority of stalkers are men (Godwin, 2003; King-Ries, 2001; Reyns, 2012; Aa, 2011). According to 2011 figures from the UK National Stalking Helpline, the majority (80%) of cyberstalking victims are female, whereas the majority (70.5%) of perpetrators are male. (According to the British Office for National Statistics (2015), twice as many women as men reported experiencing stalking between 2014 and 2015, totaling more than 1.4 million female victims. Additionally, the US Bureau of Justice Statistics (2017) found that women are at a higher risk of stalking victimisation in the United States. However, the accuracy of such numbers has been questioned due to the absence of adequate data on stalking and cyberstalking victims (Mutawa, 2016). Heinrich (2015) outlines the rationale for such victimisation and believes that women are more likely to be victims of cyberstalking than males are, owing to women's increased online time.

The extant literature indicates that stalking is a traditional crime that occurs in many parts of the world. Early literature on stalking characterises such crime related to acts or behaviours of pursuit, which is done over time, that is threatening and potentially dangerous towards the victim (Meloy, 1998; Sheridan & Grant,2007). Similarly, Thomas (1993) and Tjaden (1999) argues that stalking involves the repetitive and threatening conduct of the offender. With the advancement of the Internet, evidence revealed that traditional stalking has morphed into cyberstalking, which may be committed through any electronic devices where traditional crimes transcend into cyberspace. (Leong, 2015; Hamin & Wan Rosli, 2020). Recent literature indicates that cyberstalking is a common crime and is becoming more dangerous than traditional stalking due to the various crime stimuli of the Internet that provided tremendous

opportunities to utilise advanced computer programs (Aa, 2011; Mutawa, 2016; Hamin & Wan Rosli, 2020).

Cyberstalking has been widely defined as a repeated pursuit of an individual to intimidate, control, monitor their victims via the Internet, and its behaviours would include persistent, unwanted, premeditated, and aggressiveness (Pittaro, 2007; Reyns et al., 2012; Piotrowski & Lathrop, 2011; Reyns, Henson, & Fisher, 2012; Roberts, 2008; Sheridan & Grant, 2007; Strawhun et al., 2013). Extant scholars highlighted that the complex conceptualisation and the variation of the legal definition of stalking make it challenging to assess how can the criminal justice system respond to this offence, even with legislative refinements and effective stalking public policies in place (Brady & Nobles, 2017; Carter, 2016; Miller, 2001; Spitzberg & Cupach, 2007; Tjaden, 2009; Bouffard et al., 2021). Furthermore, the complexity of behaviours required to meet the definition outlined under anti-stalking laws had led to confusion in identifying and responding to the crime (National Center for Victims of Crime, 2008; Tjaden, 2009; Bouffard et al., 2021).

The unique circumstances in the prosecution of stalking are when the victims themselves are often asked to document and present their evidence of this behaviour's repeated nature and the emotional impact experienced (Bouffard et al., 2021). Furthermore, the under-reporting by victims and under-recording by police combined with frequent unresponsiveness of prosecutors and judges leads to significant barriers for effective criminal justice responses to stalking offences. Todd et al. (2021) highlighted that the digital footprint of victims and perpetrators is often overlooked in police investigations. Determining the technologies involved is essential for such risk assessment for earlier intervention to prevent the escalation of stalking behaviour. Intimate Partner Stalking (IPS) is loosely associated with abusive relationships, which occurs in various forms, including surveillance, confrontations, repeated communications, and threats. IPS is often present in stages where relationships deteriorate. Reports highlighted that more than half of women experience IPS in the post-breakup stage of the relationship. Bouffard et al. contended that stalking cases remain rarely prosecuted despite increasing awareness and provisions for enhanced penalties.

Regulating Cyber Stalking in Malaysia

In Malaysia, the law that may regulate cyberstalking comprises of the Communication and Multimedia Act 1998 (CMA 1998) and the Penal Code. Section 233 of the CMA 1998 governs the improper use of network facilities or network services. A person who commits an offence under this section shall on conviction be liable to a fine not exceeding fifty thousand ringgit or imprisonment for a term not exceeding one year or both. A person can also be further fined for one thousand ringgit for every day during which the offence continued after the conviction. However, no such cases relating to cyberstalking have ever been prosecuted under this section. The only case that is reported on this section is the case of Rutinin b Suhaimin v PP (2014) 5 MLJ 282 whereby the accused had published a comment that ‘Sultan Perak sudah gila !!!!!’ via his Internet account. The decision, in this case, was overturned by the higher court as there was evidence that other persons could access the accused's account as his IP line was on continuous login the whole day on the day the crime was committed. Despite the utility of Section 233 in governing cyberstalking, it does not provide the necessary protections for the victims such as the protection order, restraining order, injunction and civil remedies which are provided under the Protection from Harassment Act 1997 (PHA1997) in England and Wales. Also, this section does not identify or define the acts and behaviours that constitute cyberstalking or provide any instances of the impact of the stalkers’ behaviour on the victim such as those provided under Sections 2A and 4A of the PHA 1997.

Section 503 and 506 of the Penal code which provides for criminal intimidation may also govern cyberstalking. Criminal intimidation is committed when a person threatens another with an injury to his person with the intent to cause alarm to that person. The punishment for criminal intimidation under Section 506 is imprisonment for a term that may extend to two years or fine or both. To date, 11 cases of criminal intimidation have been prosecuted in the courts, but none of those cases involves stalking or cyberstalking. In the Singaporean case of PP v Colin Mak Yew Loong (2013, Unreported), the defendant who has been sending the victim threatening e-mails and voice messages for more than 6 years, including threats of violence by using an Ak-47 rifle and a lead pipe, was charged for criminal intimidation and was sentenced to three years of imprisonment and SGD5000 fine. This case happened before the implementation of the Protection from Harassment Act 2014 (PHA 2014) in Singapore. If the case were decided in Malaysia, the same decision would apply as criminal intimidation in Singapore is in pari materia with Section 503 of the Malaysian Penal Code. However, if the case were decided post-PHA 2014, the defendant would have been charged with cyberstalking under section 7 of the PHA 2014 whereby on conviction the accused can be liable for a fine not exceeding SGD5,000 and imprisonment not exceeding the term of twelve months or both. If the harassment towards the victim continues, the accused may also be charged for a subsequent offence with a maximum fine of SGD10, 000 or a maximum jail term of two years or both.

Parliament had recently amended the Domestic Violence (Amendment) Act 2017, which introduced an Emergency Protection Order (EPO) that allows social welfare officers to grant the victims immediate protection against their abusers (Ministry of Women, Family and Community Development, 2017). The victims need not make a report to the police or a court order to obtain the EPO which is valid for seven days (Section 3A Domestic Violence (Amendment) Act 2017). There is also the Interim Protection Order (IPO) under section 4 of the new Domestic Violence (Amendment) Act 2017, whereby victims are required to lodge a police report for the IPO to be granted. However, such legal protection against the abusive stalkers is only available to victims who are in marital and familial relationships. Therefore, such protection is not holistic and does not provide full protection for the numerous cyberstalking victims who are outside such a relationship.

MYStalk Alert

The MY Stalk Alert Apps was developed in view of facilitating and aiding victims of cyber stalking and also victims of any type of harassment in recording and collecting important evidences to ease investigation and prosecution on the part of the law enforcement. The main reason of under reporting and under-recording of cases of cyberstalking is the lack of response of the criminal justice system on the crime (Wan Rosli & Hamin, 2020). This Apps has several useful features which includes easy to understand explanation on the law governing cyberstalking, mental health support and quick checklist on identifying risks of mental health. The App also offers a novel feature of "Stalking Diary" which helps victims record and report their stalking incidences including automatic date and location generation. Apart from that, the app contains a victim support features where important emergency contacts can be inserted and automatically go on speed dial when the button is activated. This feature is important in order to ensure the victim's safety and location.

2. METHODOLOGY

In a cross-sectional study, a mixed-method design was used to collect quantitative and qualitative data from the users of the MYStalk Alert application. One of the important ways to

strengthen a study design is through triangulation, or the combination of qualitative and quantitative approaches in the study of a situation or a certain phenomenon. The researchers triangulate the two methods to check on the accuracy of the data gathered by each method, to make the choices available more concrete, to amplify strengths and lessen weaknesses in a study, and to answer broader and more complete range of research problems. For this paper, the preliminary findings are based on the primary and secondary data collection, and this stage is divided into two phases. The first phase is the library-based research or the literature review stage (Bell, 1987). All the relevant literature on cyberstalking, the legal position, and the said crime impact, criminal justice response and motivations were examined. While the primary sources involve the CMA 1998 and the Penal Code, the secondary sources include textbooks, academic journal articles, government reports, newspaper articles and online databases and sources.

The second phase of the data collection is the fieldwork, in which the primary data is mainly generated from the face-to-face semi-structured interviews with the twenty respondents. Bertaux (1981) and Guest, Bunce, and Johnson (2006) suggest that fifteen respondents would be the minimum sample size for qualitative research. The respondents of this research comprised officers from the Royal Malaysian Police, CyberSecurity Malaysia, the Malaysian Bar Council representative, the Deputy Public Prosecutors from the Attorney General Chambers, legal practitioners and an NGO (Women Aid Organisation). Such an interview method was chosen as it allows the researcher to explore the respondents' opinions of the said issues in-depth, rather than to test their knowledge or only to categorise it (Matt, 2000). The quantitative approach will be conducted by using a survey through questionnaires to more than 200 users. The sampling technique will be through random sampling. The sampling method in this research is purposive sampling, where the respondents were selected because they were likely to generate valuable data for the research (Crouch and McKenzie, 2006).

The qualitative data analysis was conducted through thematic and content analysis, in which the observations and the interview transcripts from the semi-structured interviews were examined (Seidman, 2006). The process consisted of creating codes and categories, considering the themes, analysing the respondents' perceptions and experiences, and the literature review. The primary data were triangulated with the semi-structured interview data obtained from an officer from the Ministry of Communication and Multimedia and another officer from the Ministry of Women, Family and Community Development. The said interviews were digitally recorded, and their contents were later transcribed and analysed using the Atlas. Ti qualitative research software (Friese, 2014). Triangulation is seen as traditional viewpoint in which quantitative and qualitative research are combined to reached so that they can be mutually corroborated.

3. RESULTS AND DISCUSSION

Legal Response to Cyberstalking

According to the evidence, the majority of the respondents (12 out of 18) believed that the legal response against cyberstalking is inadequate. The impression is consistent with local literature, which claims that Malaysia's criminal justice system provides minimal to stalking victims. Several respondents, on the other hand, puts the responsibility to the victims in collecting evidence to ensure easy prosecution A respondent from an enforcement agency remarked that:

The victim needs to keep a copy of the report to ensure a trail of evidence for easy reference in case the police need to investigate in the future.

Similarly, one respondent agreed with the importance of keeping evidence and reporting to the authorities, namely the police and the MCMC, to have trails of evidence of cyberstalking experienced by the victim. The respondent stated that:
Victims must always report their stalkers to the police or the MCMC.
To be more proactive and aware of stalking incidents, a respondent from an NGO proposed that victims should periodically report and update the authorities on their cyberstalking experiences. The necessity of reporting to relevant authorities was to give police with crime statistics because if victims did not complain, the police would have no record of the incidents and cyberstalking would not be considered a serious crime. The respondent remarked that:
The victims should always report to the police as it gives the police a chance to be more proactive and take suitable actions against the stalker.
However, from the victim's point of view, the belief was that it was a futile exercise as police responses were not forthcoming. One victim argued that:
I've filed multiple police reports throughout the last six months, but the cops have been reluctant to intervene. I even filed a police report about the stalker following me around, and the stalker was standing outside the police station when I filed it. Nothing, however, was done. I'm not in the least bit secure.

Documenting incidences as Trail of Evidence
Contrary to the Malaysian legal position, other jurisdictions such as England and Wales provide avenues for the police to keep track of stalking incidences faced by victims. Such avenues are in the form of a 'PIN' or Police Information Notice where victims can report stalking incidence to the police. The report is kept for future reference to provide a clear trail of evidence. The findings revealed that majority of the respondents (87 percent) believed that MY Stalk Alert have the potential to aid victims of stalking in documenting relevant evidence in helping with investigation. However, there are a minority of respondents (2.3 percent) feel that the App is unhelpful in helping stalking victims. One respondent stated that :
I find the Application to be very helpful especially in terms of collecting evidence.
Another respondent highlighted that:
It's a good application in helping us to document incidences.
The literature suggested that cyberstalking victims who experienced serious offences were not likely to engage with anyone to report or seek help as they were ashamed of the incidents (Fissel, 2021). Venkatasubramaniam (2021) in his paper examining technologies in empowering Individual with Intellectual and Development Disabilities, who face abuses if they exposed or reported any incidents, highlights that a self-reporting tool is an exciting idea as it does not only help in recording incidents but protect the victims from any form of stigmatization. This situation is similarly observed among stalking victims. The survey conducted suggested that 88% of My Stalk Alert users find the apps helpful in documenting stalking incidents. Additionally, the survey conducted on the commercialization of the apps suggested that the user has not used any self-reporting tools or apps before My Stalk Alert. A stunning 95% of the respondents indicate that they have no experience encountering similar apps in Malaysia that offer the platform to record and report cyberstalking incidents.

The Novelty and Unique Characteristic of the MY Stalk Alert Application
On the application's novelty and unique requirements, the majority of the respondents, (95%) highlighted that the application enables victims of cyberstalking and harassment to document proof and keep track of their activities. Additionally, this application is unique from other existing market offerings in that it is concerned with the well-being of the individual and victim

of stalking crime and contains a first aid kit for self-assessment of victims' mental health. Finally, this application includes a set of proprietary criteria for documenting stalker activities that can be shared with criminal justice organisations for reporting purposes. On this point, majority of the respondents noted that the application provides various features that aids victims of stalking and cyber stalking. One respondent stated that:
The features of this application is very good and I have never used any apps that have such features as this app.
Other respondents noted that they are not any aware any application that have similar features with MYSTALK Alert. One highlighted that:
No, I have not used any similar apps and don't know of any other apps with MSA's features.

Impact & Usefulness of MY Stalk Alert Application
MY Stalk Alert was designed to assist at least three parties: application users, law enforcement agencies, and the legislators. The majority feedback gathered from the user's experience indicated the fulfillment of its purpose of assisting and providing support to victim of stalking. In addition, the user feedback on this application could be used by the Parliament to enact a specialized anti-stalking statute. A total of 83.7 percent of users stated that this application is helpful, straightforward, and serves its goal, and a total of 88.9% are highly confident in utilizing MY Stalk Alert to gather evidence and receive the aid they needed. Among the responses received from users of this application, pertaining to its impact and usefulness includes:
"I have no issues with the app. The app simple to use, concise and helpful for those who have experience stalking."
Another respondent highlighted that:
"In my opinion, this is a great apps as I have personal experience encountered with stalker online. It really does help me."

4. DISCUSSION

The preceding findings indicated that due to the insufficient response by the criminal justice system, specifically the police, resulted in under-reporting of the crime. On the one hand, the findings underscored the critical nature of reporting cyberstalking incidents to the police in order to guarantee a trail of evidence exists to facilitate an investigation. This perspective is consistent with the literature on cyberstalking, which encourages victims to disclose their stalking experiences to appropriate authorities to expedite the criminal justice process. On the other hand, victims' perceptions indicate that the majority are extremely hesitant to disclose, believing that reporting would result in the harassment continuing. This impression is also consistent with recent research indicating that underreporting is a result of the criminal justice system's unresponsiveness. This under-reporting prompted the researchers to create an app to assist victims in reporting crimes. Such elements within the App will aid in the documentation of evidence and will also provide legal and psychological support to victims. Additionally, such application, if made available will aid the various stakeholders mainly the legislators, enforcement agencies, and users.

5. CONCLUSION

The findings indicate that MY Stalk Alert does not only help victims in recording incidences of stalking within a touch of a button, additionally, such application also aids victims in

conducting self-assessments on mental health and make available the SOS button in case of emergency. Such features within the application have impacted victims which finds it easier to record and report their stalking incidences. The App also proves to be unique and novel as it is the first of its kind, made available to Malaysian users. My Stalk Alert acts as a response to the fight for the effective criminalization of stalking in Malaysia. Legal protection should be accessible to all of those in need, illustrating the necessity for a specific law to govern such crime. The Malaysian legislation that may be utilised to deal with cyberstalking is in dire need of immediate reform, which instrumentally may be in the form of an amendment to the Penal Code to include specific provisions for stalking and cyberstalking. Another idealistic form would be a stand-alone Act, which criminalises cyberstalking. In the long run, the absence of specific legislation may pose severe mental and psychological impacts on the victims. The third victimization of their friends and family will also impact the nation. Malaysia should follow the footsteps of the UK to continuously enhance and review the anti-stalking legal framework to criminalise cyberstalking and holistically provide adequate legal protection for the victims.

Acknowledgement
This work was supported by research grant FRGS/1/2019/SSI10/UITM/02/2 by the Research Management Centre, UiTM Shah Alam, Selangor, Malaysia.

6. REFERENCES

[1]. Ahlgrim, B., & Terrance, C. (2021). Perceptions of Cyberstalking: Impact of Perpetrator Gender and Cyberstalker/Victim Relationship. Journal of Interpersonal Violence, 36(7–8), NP4074–NP4093. https://doi.org/10.1177/0886260518784590

[2]. Bertaux, D. (1981). From the Life-History Approach to The Transformation of Sociological Practice. Biography and Society: The Life History Approach in The Social Sciences 29–45. London: Sage.

[3]. Bouffard, L. A., Bouffard, J. A., Nobles, M. R., Askew, L. (2021). Still In The Shadows: The Unresponsiveness Of Stalking Prosecution Rates To Increased Legislativeattention. Journal of Criminal Justice,Volume 73,2021,101794,ISSN 0047-2352,https://doi.org/10.1016/j.jcrimjus.2021.101794.(https://www.sciencedirect.com/science/article/pii/S0047235221000143)

[4]. Crouch, M., McKenzie, H. (2006). The Logic of Small Samples in Interview-based Qualitative Research. Social Science Information. Vol. 45 No. 4 pp: 483-499.

[5]. Fissel, E.R. (2021). Victims' Perceptions of Cyberstalking: An Examination of Perceived Offender Motivation. Am J Crim Just (2021). https://doi.org/10.1007/s12103-021-09608-x

[6]. Guest, G., Bunce, A., Johnson, L. (2006). How Many Interviews Are Enough? An Experiment with Data Saturation and Variability.Field Methods. Vol. 18 No. 1 pp: 59-82

[7]. Halder, D., Jaishankar, K. (2011). Cyber Gender Harassment and Secondary Victimisation: A Comparative Analysis of the United States, the UK, and India. Victims & Offenders, 6:4, 386-398, DOI: 10.1080/15564886.2011.607402

[8]. Hamin, Z., Wan Rosli, W.R. (2017). Managing Cyberstalking in Electronic Workplaces. International Conference on Business and Social Science (ICoBSS). 20 February 2017 – 1 March 2017, Universiti Teknologi MARA Melaka, Melaka Malaysia.

[9]. Indramalar, S. (2017, 24 March). Crossing the Line. The Star. Retrieved at https://www.pressreader.com/malaysia/the-star-malaysia-star2/20170324/281479276240629.
[10]. Jaishankar, K. (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour. Florida: Taylor & Francis Group.
[11]. Todd, C., Bryce, J., Franqueira, N. L. (2021). Technology, cyberstalking and domestic homicide: informing prevention and response strategies. Policing and Society, 31:1, 82-99, DOI: 10.1080/10439463.2020.1758698
[12]. Wright, M. F. (2018). Cyberstalking victimisation, depression, and academic performance: the role of perceived social support from parents. Cyberpsychology, Behavior, and Social Networking, 21(2), 110-116.